International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6941
***Article Received**: 29 March 2023 **Revised**: 14 May 2023 **Accepted**: 26 May 2023*

Intrusion Detection System using the Hybrid Model of Classification Algorithm and Rule-Based Algorithm

Abhijit Kadam[1], Bindu Garg[2], Milind Gayakwad[3], Rahul Joshi[4], Ketan Kotecha[5]
[1]Bharati Vidyapeeth Deemed to be University, College of Engineering,
Pune, India
e-mail: abhijit.b.kadam@bharatividyapeeth.edu
[2]Bharati Vidyapeeth Deemed to be University, College of Engineering,
Pune, India
e-mail: bgarg@bvucoep.edu.in
[3]Bharati Vidyapeeth Deemed to be University, College of Engineering,
Pune, India
e-mail: mdgayakwad@bvucoep.edu.in
[4]Symbiosis Institute of Technology, Symbiosis International (Deemed University),
Pune, India
e-mail: rahulj@sitpune.edu.in
[5]Symbiosis Institute of Technology, Symbiosis International (Deemed University),
Pune, India
e-mail: head@scaai.siu.edu.in

Abstract— Intrusion detection system ID is necessary to secure the system from various intrusions. Analysis of the communication to categorize the data as useful or malicious data is crucial. The cyber security employed using intrusion detection systems should not also cause the extra time to perform the categorization. Nowadays machine learning techniques are used to make the identification of malicious data or an intrusion with the help of classification algorithms. The data set used for experimenting is KDD cup 99. The effect of individual classification algorithms can be improvised with the help of hybrid classification models. This model combines classification algorithms with rule-based algorithms. The blend of classification using machine and human intelligence adds an extra layer of security. An algorithm is validated using precision, recall, F-Measure, and Mean age Precision.

The accuracy of the algorithm is 92.35 percent. The accuracy of the model is satisfactory even after the results are acquired by combining our rules inwritten by humans with conventional machine learning classification algorithms. Still, there is scope for improving and accurately classifying the attack precisely.

Keywords- Rule-Based Algorithm, Intrusion Detection System, Hybrid Model.

I. INTRODUCTION

Data security and privacy are important measures in ensuring the Machine's security. Cyber Security, Computer Forensics, and Cyber Laws deal with securing the system and analysis of the Attack incurred if any[1], [2]. Analysis helps in detecting the preventing the loss of Information and other resources. The use of social media forums, software, apps, and electronic gadgets carries valuable data. This data is compromised if the intruder gets access to the system. The intrusion detection system is necessary to address similar issues. The conventional may not work appropriately. The way of attack, the identity, and the severity change over time. [3]

Machine Learning facilitates the identification of the attack and training of the system to cope with the abnormalities in the system, The models comprise classification techniques, Regression techniques, a Combutronic network, and a Memory model. Each of the models and their combination helps in implementing the Intrusion Detection System[4]. For example, the regression algorithm may figure out the RAM consumption and ROM in the normal condition by identifying some thresholds. Classification algorithms can identify the threats by looking at the stored identity of the intrusion[5].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6941
***Article Received**: 29 March 2023 **Revised**: 14 May 2023 **Accepted**: 26 May 2023*

- **Intrusion detection system**

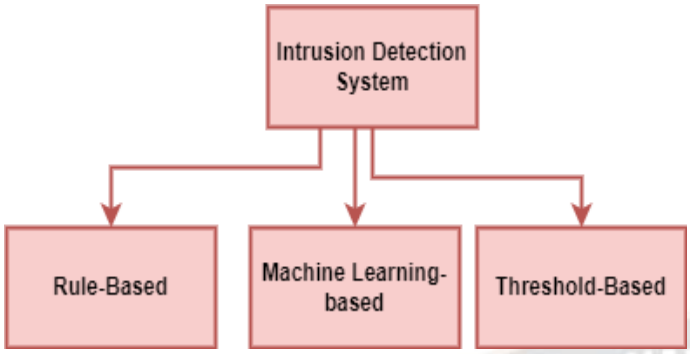

Figure 1. Types of Intrusion Detection System

Fig. 1 states that there are three categories of the solution to address the Intrusion Detection System (Mainly)[6], [7]. These techniques are Rule-Based techniques, Machine Learning-Based techniques, and Threshold-based techniques[8]. The proposed model uses the Rule-based technique and machine learning technique as a part of the Model. The rules are designed specifically for detecting intrusion, whereas enhancement over the conventional model helps to achieve accuracy in detecting the intrusion[9].

The contribution of the research work is as below.

- Design of the model based on the Rule based + Hybrid approach.
- Improvisation of the accuracy using the novel approach.

Section 2 covers the Literature Survey, detailed analysis of the datasets, algorithms, models responsible for the detection of the intrusion. Section 3 Materials and Methods covers the approach used in general and detailed computation carried out during the classification. The phases like data collection, pre-processing, Rule based Model, Hybrid Model, Distribution of the weights, Validation is discussed in detail. Section 4 deals with results

TABLE I. DIFFERENT DATASETS

DATA SETS	DATASET		
	Data	***Source***	***specifications***
1	KDD CUP-99	http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html	Attacks on military equipment for intrusion detection [29][30][31]
2	NSL-KDD	https://github.com/jmnwong/NSL-KDD-Dataset,	Differentiation between good and bad [32][33] connections [34][35][36].
3	CICIDS2017	https://www.unb.ca/cic/datasets/ids-2017.html	CICFlowMeter is used to create data resembling the real world, has 80 features, and data traffic is of 5 days [36][37][38].
4	LuFlow Dataset	https://www.kaggle.com/datasets/mryanm/luflow-network-intrusion-detection-data-set[39][40]	One day data, Cisco Joy Meter [41][42] is used to collect features in coordination with Cyber Threat [43] Intelligence, Lancaster University [44][45][46]

gathered during the pre-processing, Feature extraction, Comparative analysis with other algorithms. The ROC curve, histogram, Correlation, tabulated form helps in understanding the output of the experiment. Section 5 concludes the paper by providing brief conclusive remarks.

II. TYPE STYLE AND FONTS

Wherever A literature survey of various models and datasets was conducted. The details about the dataset and as mentioned below.

The standard dataset for the experimentation is mentioned in the table below. There are datasets like KDDCUP-99, NSL-KDD, CICIDS2017, CAIDA, UNSW_NB15, and Ludlow Dataset [27][28].

Also, there are datasets like ADFA-WD, CAIDA, and UNSW_NB15 which also provide important data associated with Intrusion Detection[9]–[14].

The author used the WSN-KNN approach [15] to apply the intelligent detection algorithm for the Internet of Things. The PL-AOA (Arithmetic Optimization Algorithm). The improvement in the KNN classification makes the Algorithm robust to deal with DoS attacks. The experiment is performed on WSN-DS. The author uses LSTM and GRU [16] to provide the hybrid effect for avoiding car hacking. The important novel outcome of the approach is less response time. The DDoS dataset is used for applying the hybrid model. The research [17] was carried out using a novel Arithmetic Optimization Algorithm (AOEDBC-DL) based on the binary LSTM and deep learning approach[46]. The accuracy is 98.16 % for the WSN-DS dataset. [18] proposes the MQTT model based on the queuing theory, the accuracy of this model is 99.92 %. The MQTT model uses Machine Learning and other Deep Neural Network models. [19] proposed a novel dataset for the identification of the intrusion[20], [21]. The accuracy of the dataset is 99.64%. The results are validated using training, testing accuracies[47], and performance comparison with the XGBoost algorithm. [22] refers to the evolvement of the attacks and the possible ways to mitigate the effect of the attack. Information about the statistics related to the packets and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6941
***Article Received**: 29 March 2023 **Revised**: 14 May 2023 **Accepted**: 26 May 2023*

automatic and manual approaches to deal with the intrusion is mentioned[48]. [23]A literature survey about the intrusion detection system is performed. The study covers brief information about the dataset, algorithm, and accuracies[24]–[26].

III. MATERIALS AND METHODS

Intrusion Detection System Model – The proposed Architecture to classify the intrusions.

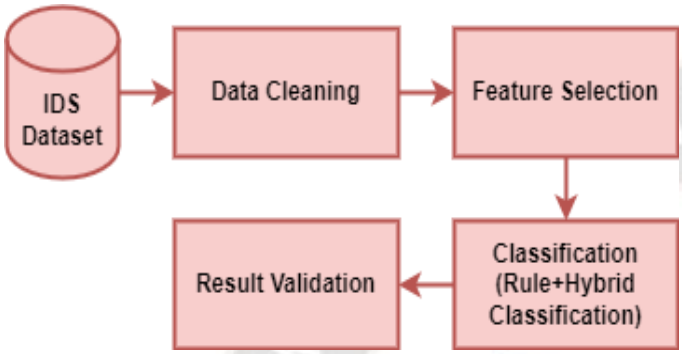

Figure 2. Architecture of Intrusion Detection System using Hybrid- Rule-based Model.

The phases involved in the entire Intrusion Detection System mentioned in Fig. 2 are as mentioned below-
Data Collection, Normalization of data, Pre-processing, Analysis of data, Rules formation, Feature Extraction, Hybrid classification, and Validation of a Model[9]–[13].

A. Data Collection-

The dataset of is generated using JOY along with the server at the department. The data is converted to a structured format so that it can be pre-processed as per the requirements.

3.2. Pre-processing

Data is converted to a structured format. The type of data is identified distribution is verified. The impurities in the data are recognized by checking the missing values, punctuation, links, and dates and are converted into the appropriate format so that they can be processed [9]–[11].

B. Validation of Data

Learning is possible if the data is distributed in a normal format. If the distribution is not normal, it is expected to be normalized. The testing of the validity is necessary. The validation of each feature is performed, and thereafter the entire dataset is validated.

C. Feature Extraction

The prominent features are shortlisted manually based on their usage. The dataset contains the link, which is least relevant concerning learning. Also, the automated process of shortlisting the features was employed. The correlation matrix is plotted for analyzing the association among the features. The top 8 features are shortlisted based on the correlation.

D. Classification (SVM (Support Vector Machine), LR (Logistic Regression), DT (Decision Tree))

The given problem is the classification problem. There are three classification algorithms shortlisted based on the 7 different classification algorithms that were examined Support Vector Machine, Logistic Regression, and decision tree are used.

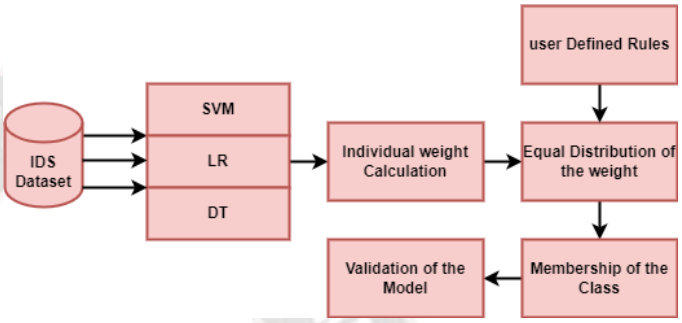

Figure 3. Computational model of Intrusion Detection System

The computational model as indicated in Fig.3 conveys the detailed functioning of the Intrusion Detection System. The data is collected from the IDS (Intrusion Detection System) Dataset. Three different classification algorithms employed Support Vector Machine (SVM), Linear Regression (LR), and Decision Tree (DT). The weight of individual algorithms is identified by equally distributing the load amongst the three algorithms. The Rules are explicitly defined to channel the specific form of traffic. To design the rules SNORT is used. The hybrid model with weight can decide the membership of the class. Thus, the Novel approach to classifying the data is based on the Collective response of the three baseline algorithms and user-defined rules. The results are validated using the testing dataset (30%). Precision, Recall, F-Measure, True Positive Rate, and True Recall Rate are calculated. The specificity and Sensitivity are calculated. The curve based on the collected data is plotted. The graphs are plotted to know the correlation, ROC Curve, and distribution of the data.

The parameters used for the Intrusion Detection system were formulated using the JOY utility of the CISCO. The details are as mentioned in Table 2.

TABLE II. FEATURES COLLECTED USING JOY.

Features	Description
SOURCE_IP	IP (Internet Protocol) Address of the Source Machine.
SOURCE_PORT	The port number of the source Machine.
DESTINATION_IP	The IP address of the destination.
DESTINATION_PORT	The destination addresses of the Machine.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6941
***Article Received**: 29 March 2023 **Revised**: 14 May 2023 **Accepted**: 26 May 2023*

PROTOCOL	The type of protocol (with the flow of packets)
BYTES_IN	The number of bytes (Inward)
BYTES_OUT	The number of bytes (Outword)
NUMBER_PACKETS_IN	Number of packets (Inward)
NUMBER_PACKETS_OUT	Number of packets (Outward)
ENTROPY	Several bits introduced is 8 bits.
TOTAL_ ENTROPY	The entropy across the data.
MEAN_IPT	Mean of inter-packet arrival
TIME_START	START TIME in seconds
TIME_END	END TIME in seconds
DURATION	The total duration
LABEL	BENIGN, OUTLIER, MALICIOUS

Fig. 4 shows the relation between the flow of the packets between the source and destination port. The flow of the traffic can be interpreted by looking at the pattern of the scattered data. The concentration is almost parallel across the axes.

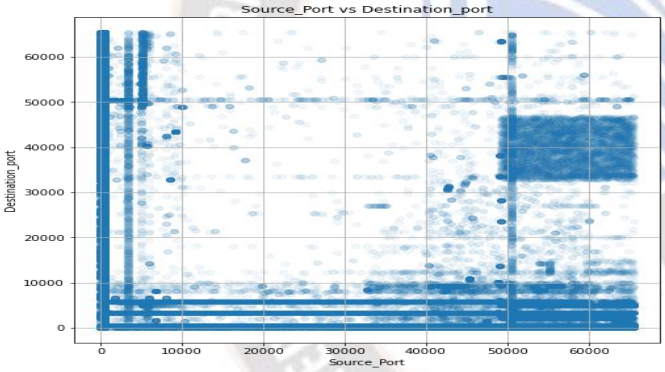

Figure 4. Correlation of Source Post and Destination Port

There are very a small number of packets found at the diagonal.

IV. RESULT

Figure 5 shows the relation between the Flow of the Bytes Outside and the flow of the bytes inside. The correlation is dense to the size of 10,000 and it becomes sparse after 60,000 bytes. Though there is a moderate flow of the bytes from 10,000 to 50,000. This conveys the specific form of the pattern while data is transmitted.

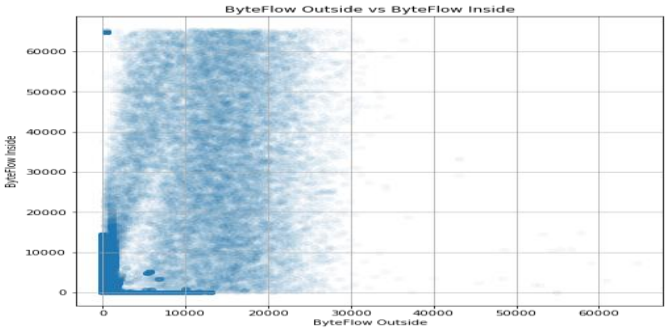

Figure 5. States the distribution of the individual feature

As mentioned in Fig.5 the form of a histogram. The histogram helps in understanding the presence of skewness in the data. Fig.6 states that the data is not normally distributed so, the remedial action helps in drifting the skewed data to normal.

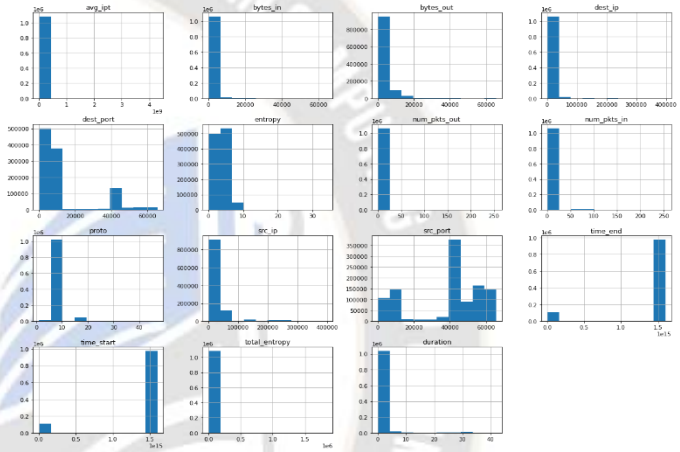

Figure 6. Distribution of the data for each Feature

The distribution of Features like Destination Port, Source Port, and Entropy is close to normal. While the distribution of the Features namely bytes in, bytes out, destination IP, number of packets in, number of packets out, and total entropy are representing the skewness at left. Some features like time_start and time_end represent the skewness at right.

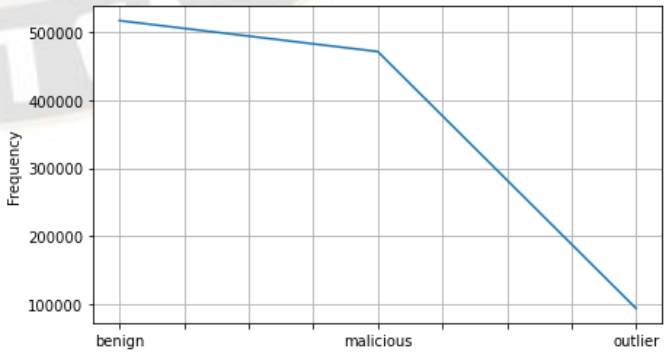

Figure 7. The outlier and Malicious data identification

Fig.7 states the fact about the presence of outliers is dropping as the frequency drops from 500000 to 100000. The malicious

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6941
***Article Received**: 29 March 2023 **Revised**: 14 May 2023 **Accepted**: 26 May 2023*

data is at its peak when the frequency is approximately 4,80,000. The presence of benign is less harmful.

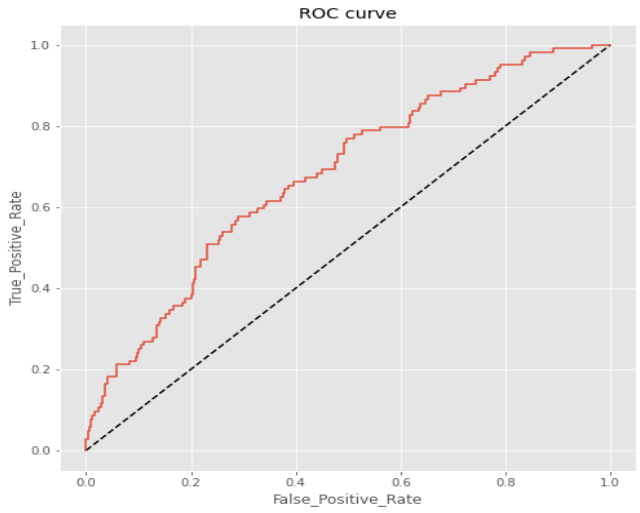

Figure 8. Figure 8: Receiver Operating Characteristic Curve

ROC helps understand the classifier's performance with varying effects of the threshold. Figure 8 states that the graph of True_Positive_Rate is plotted against False_Positive_Rate. The graph can be interpreted. The graph reveals the resilience of the classification mechanism. The performance does not degrade with an increase in the value of the threshold.

Table no.3 indicates the comparison among individual classification, hybrid classification, and Rule-Based hybrid approaches. The performance is increased using Hybrid Model and further enhancement in the accuracy is possible because of the Rules.

TABLE III. COMPARATIVE ANALYSIS

Sr. No.	Algorithm/Approach	Accuracy
1	SVM	78.22
2	LR	69.25
3	DT	76.33
4	XGBOOST	82.45
5	Hybrid Model	91.29
6	Rule-Based Hybrid Model	92.35

V. CONCLUSION

The result of the hybrid rule-based classifier is adequate. The accuracy of the algorithm is 91.29 %. The comparative Analysis is performed concerning the existing classification algorithm. The racy of the classification remains intact even if the threshold values are increased or decreased. The Novel approach further improvises the performance of the classification algorithm by adding the rule specifically designed for the given environment, so the accuracy is boosted to 92.35 %. The distribution, ROC curve, comparative analysis, and outlier detection prove the performance of the Approach. There is scope for further improvement of the performance of different datasets. The base algorithms can be rigorously experimented with to check their robustness.

ACKNOWLEDGMENT

I acknowledge the help and support given by the research guide Dr. Bindu Garg. This research was funded by "Research Support Fund of Symbiosis International (Deemed University), Pune, Maharashtra, India".

REFERENCES

[1] A. A. Rao, P. Srinivas, B. Chakravarthy, K. Marx, and P. Kiran, "A Java Based Network Intrusion Detection System (IDS)," Proc. 2006 IJME - INTERTECH Conf., pp. 1–8, 2006.

[2] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems," J. Inf. Secur. Appl., vol. 58, no. February, p. 102717, 2021, doi: 10.1016/j.jisa.2020.102717.

[3] S. R. Snapp, S. E. Smaha, D. M. Teal, and T. Grance, "The DIDS (Distributed Intrusion Detection System) Prototype," Proc. Summer USENIX Conf., pp. 227–233, 1992, [Online]. Available: https://www.usenix.org/legacy/publications/library/proceedings/sa92/snapp.pdf

[4] B. Garg, "Scheme of Neural Network for Time Series Analysis," no. October 2008, 2015.

[5] B. Garg and R. Garg, "Enhanced accuracy of fuzzy time series model using ordered weighted aggregation," Appl. Soft Comput. J., vol. 48, no. January 2016, pp. 265–280, 2016, doi: 10.1016/j.asoc.2016.07.002.

[6] C. Clark, W. Lee, D. Schimmel, D. Contis, M. Koné, and A. Thomas, "A Hardware Platform for Network Intrusion Detection and Prevention," Netw. Process. Des., pp. 99–118, 2005, doi: 10.1016/B978-012088476-6/50007-1.

[7] D. K, "Anomaly based Network Intrusion Detection System Dinakara K Anomaly based," Engineering, 2008.

[8] Mike Peeters, "Designing and Deploying Intrusion Detection Systems," Cisco, 2003, [Online]. Available: https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/Designing_and_Deploying_ids_technologies.pdf

[9] library of congress cataloging-in-publication Data, Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort , Apache , MySQL , PHP , and ACID B RUCE P ERENS ' O PEN S OURCE S ERIES. 2003.

[10] S. Axelsson, "Paper.IDS - A Survey and Taxonomy," pp. 1–27, 2000, [Online]. Available: papers3://publication/uuid/89f1c9ad-ad04-4684-a05e-f94f128ce4fc

[11] B. Garg, "Optimizing Number of Inputs to Classify Breast Cancer Using Artificial Neural Network," J. Comput. Sci. Syst. Biol., vol. 02, no. 04, 2009, doi: 10.4172/jcsb.1000037.

[12] B. S. Kumar, T. C. S. P. Raju, M.Ratnakar, S. D. Baba, and N.Sudhakar, "Intrusion Detection System- Types and Prevention," Int. J. Comput. Sci. Inf. Technol., vol. 4, no. 1, pp. 77–82, 2013.

[13] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, "An Enhanced Intrusion Detection Model Based on Improved kNN in

WSNs," Sensors, vol. 22, no. 4, pp. 1–18, 2022, doi: 10.3390/s22041407.

[14] S. Ullah et al., "HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles," Sensors, vol. 22, no. 4, pp. 1–20, 2022, doi: 10.3390/s22041340.

[15] F. Alrowais et al., "Intelligent Intrusion Detection Using Arithmetic Optimization Enabled Density Based Clustering with Deep Learning," Electronics, vol. 11, no. 21, p. 3541, Oct. 2022, doi: 10.3390/electronics11213541.

[16] M. A. Khan et al., "A deep learning-based intrusion detection system for mqtt enabled iot," Sensors, vol. 21, no. 21, pp. 1–25, 2021, doi: 10.3390/s21217016.

[17] K. Kotecha et al., "Enhanced network intrusion detection system," Sensors, vol. 21, no. 23, pp. 1–15, 2021, doi: 10.3390/s21237835.

[18] K. K. Beldar, M. D. Gayakwad, D. Bhattacharyya, and T. H. Kim, "A comparative analysis on contingence structured data methodologies," Int. J. Softw. Eng. its Appl., 2016, doi: 10.14257/ijseia.2016.10.5.03.

[19] M. A. Boukhari and M. D. Gayakwad, "An experimental technique on fake news detection in online social media," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 8 Special Issue 3, 2019.

[20] J. McHugh, "Intrusion and intrusion detection," Int. J. Inf. Secur., vol. 1, no. 1, pp. 14–35, 2001, doi: 10.1007/s102070100001.

[21] A. Kadam and B. Garg, "Accuracy and Deviation Analysis of Intrusion Detection System," SSRN Electron. J., 2022, doi: 10.2139/ssrn.4025358.

[22] G. Smith, "Public Sector Open Innovation: Exploring Barriers and How Intermediaries Can Mitigate Them," Thesis, no. September, 2018.

[23] M. S. O'Hern and L. R. Kahle, "The Empowered Customer: User-Generated Content and the Future of Marketing," Glob. Econ. Manag. Rev., vol. 18, no. 1, pp. 22–30, 2013, doi: 10.1016/s2340-1540(13)70004-5.

[24] M. Mayrhofer, J. Matthes, S. Einwiller, and B. Naderer, "User generated content presenting brands on social media increases young adults' purchase intention," Int. J. Advert., vol. 39, no. 1, pp. 166–186, 2020, doi: 10.1080/02650487.2019.1596447.

[25] Beldar, Kavita K., M. D. Gayakwad, and M. K. Beldar. 2016. "Optimizing Analytical Queries on Probabilistic Databases with Unmerged Duplicates Using MapReduce." Int. J. Innov. Res. Comput. Commun. Eng 4: 9651–59.

[26] Beldar, Kavita K., M. D. Gayakwad, Debnath Bhattacharyya, and Hye-Jin Kim. 2016a. "Query Evaluation on Probabilistic Databases Using Indexing and MapReduce." International Journal of Database Theory and Application 9 (10): 363–78.

[27] Beldar, Kavita K., M. D. Gayakwad, Debnath Bhattacharyya, and Tai-Hoon Kim. 2016b. "A Comparative Analysis on Contingence Structured Data Methodologies." International Journal of Software Engineering and Its Applications 10 (5): 13–22.

[28] Beldar, Miss Menka K., M. D. Gayakwad, and Miss Kavita K. Beldar. 2018. "Altruistic Content Voting System Using Crowdsourcing." International Journal of Scientific Research and Review 7 (5): 477–86.

[29] Beldar, Miss Menka K., M. D. Gayakwad, Miss Kavita K. Beldar, and M. K. Beldar. 2018. "Survey on Classification of Online Reviews Based on Social Networking." IJFRCSCE 4 (3): 55.

[30] Boukhari, Mahamat Adam, Prof Milnid Gayakwad, and Prof Dr Suhas Patil. 2019. "Survey on Inappropriate Content Detection in Online Social Media." International Journal of Innovative Research in Science, Engineering and Technology 8 (9): 9297–9302.

[31] Gayakwad, M. D., and B. D. Phulpagar. 2013. "Research Article Review on Various Searching Methodologies and Comparative Analysis for Re-Ranking the Searched Results." International Journal of Recent Scientific Research 4: 1817–20.

[32] Gayakwad, Milind. 2011. "VLAN Implementation Using Ip over ATM." Journal of Engineering Research and Studies 2 (4): 186–92.

[33] Gayakwad, Milind, and Suhas Patil. 2020. "Content Modelling for Unbiased Information Analysis." Libr. Philos. Pract, 1–17.

[34] Gayakwad, Milind, Suhas Patil. "Analysis of Methodologies to Model the Content for Conveying the Correct Information." In 2021 International Conference on Computing, Communication and Green Engineering (CCGE), 1–4. IEEE.

[35] Gayakwad, Milind, Suhas Patil ."Assessment of Source, Medium, and Intercommunication for Assessing the Credibility of Content." In 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 1–5. IEEE.

[36] Gayakwad, Milind, Suhas Patil, Rahul Joshi, Sudhanshu Gonge, and Sandeep Dwarkanath Pande. "Credibility Evaluation of User-Generated Content Using Novel Multinomial Classification Technique." International Journal on Recent and Innovation Trends in Computing and Communication 10 (2s): 151–57.

[37] Gayakwad, Milind, Suhas Patil, Amol Kadam, Shashank Joshi, Ketan Kotecha, Rahul Joshi, Sharnil Pandya, et al. 2022. "Credibility Analysis of User-Designed Content Using Machine Learning Techniques." Applied System Innovation 5 (2): 43.

[38] Harane, Swati T., Gajanan Bhole, and Milind Gayakwad. 2017. "SECURE SEARCH OVER ENCRYPTED DATA TECHNIQUES: SURVEY." International Journal of Advanced Research in Computer Science 8 (7).

[39] Kavita Shevale, Gajanan Bhole, Milind Gayakwad. 2017. "Literature Review on Probabilistic Threshold Query on Uncertain Data." International Journal of Current Research and Review 9 (6): 52482–84.

[40] Mahamat Adam Boukhari, Milind Gayakwad. 2019. "An Experimental Technique on Fake News Detection in Online Social Media." International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8 (8S3): 526–30.

[41] Maurya, Maruti, and Milind Gayakwad. 2020. "People, Technologies, and Organizations Interactions in a Social Commerce Era." In Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2018), 836–49. Springer International Publishing.

[42] Milind Gayakwad, B. D. Phulpagar. 2013. "Requirement Specific Search." IJARCSSE 3 (11): 121.

[43] Panicker, Aishwarya, Milind Gayakwad, Sandeep Vanjale, Pramod Jadhav, Prakash Devale, and Suhas Patil. n.d. "Fake News Detection Using Machine Learning Framework."

[44] Sharma, Jitin, Prashant C. Chavan, T. B. Patil, Supriya C. Sawant, and Milind Gaykawad. 2022. "A Comparative Analysis of Brain Tumor Classification and Prediction Techniques by Applying

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6941
***Article Received**: 29 March 2023 **Revised**: 14 May 2023 **Accepted**: 26 May 2023*

MRI Images Encompassing SVM and CNN with Transfer Learning Method." Journal of Algebraic Statistics 13 (3): 393–405.

[45] Alagarsamy, M. ., Shanmugam, N. ., Paramathi Mani, D. ., Thayumanavan, M. ., Sundari, K. K. ., & Suriyan, K. . (2023). Detection of Polycystic Syndrome in Ovary Using Machine Learning Algorithm. International Journal of Intelligent Systems and Applications in Engineering, 11(1), 246–253. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2464

[46] Shevale, Kavita, Gajanan Bhole, and Milind Gayakwad. 2017. "Probabilistic Threshold Query on Uncertain Data Using SVM." Int. J. Adv. Res. Comput. Sci 8: 1967–69.

[47] Singh, Mahendra Kumar, Amol K. Kadam, Milind Gayakwad, Pramod Jadhav, Vinayak N. Patil, Prasad Kadam, Vinod Patil, and Sunita Dhotre. n.d. "An empirical approach for underwater image quality enhancement and object detection using deep learning." https://www.researchgate.net/profile/Amol-Kadam-3/publication/363210290_An_Impirical_Approach_for_Underwater_Image_Quality_Enhancement_and_Object_Detection_using_Deep_Learning_An_Impirical_Approach_for_Underwater_Image_Quality_Enhancement_and_Object_Detection_using_Deep_L/links/6311901cacd814437ff7a165/An-Impirical-Approach-for-Underwater-Image-Quality-Enhancement-and-Object-Detection-using-Deep-Learning-An-Impirical-Approach-for-Underwater-Image-Quality-Enhancement-and-Object-Detection-using-Deep-L.pdf.